DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Christopher J. Lutz with Registration Number 44,883 on 04/03/2008. According to the Attorney's telephonic discussion, Applicant agreed to amend Claims 8, 19, 36, 37, 39, 40, 41, and 42.

The application has been amended as follows:

8. (Currently Amended) The method of claim 1 ~~6~~ wherein the reroute message is indicative of the filter complex receiving message traffic according to the first transport mechanism intended for the target node via the target node router serving the target node.

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial

19. (Currently Amended) A network management server for redirecting undesirable message traffic comprising:

a network intrusion detector monitor operable to receive an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

a routing processor operable to propagate routing information from a routing table database to reroute all message traffic using the first transport mechanism directed to the particular target node; and

a connection to a filter complex responsive to the routing processor, the filter complex operable to distinguish desirable message traffic from undesirable message traffic, and further operable to transmit, by redirecting the desirable message traffic via a second transport mechanism over the communications network, the desirable message traffic to the target node, the redirecting thus

Deleted: the same

transporting a particular message in the desirable message traffic via both the first transport mechanism and the second transport mechanism;
the filter complex operable to reroute all message traffic including propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node,
the routing processor operable to direct the filter complex to propagate routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism, the second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs,
the second transport mechanism defining a Virtual Private Network (VPN) protocol,
the network management server further operable to send a reroute message to the filter complex, in response to which the filter complex is operable to reroute the message traffic, the reroute message indicative of the filter complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node.

36. (Currently Amended) In a network management server of a networked system of data communications devices, a method for transparently intercepting, filtering, and rerouting message traffic for recovering from a distributed denial of service attack comprising:

detecting, at a network monitor in the network management server, a pattern of inundating undesirable message traffic to a particular target node transported via a first transport mechanism in a communications network;
receiving, via a routing processor, an indication of the undesirable message traffic directed to the particular target node;
transmitting, via a network interface, a reroute message to a filter complex having a security filter operable to distinguish desirable message traffic from undesirable message traffic; and

rerouting, via a filter routing device in the filter complex, all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filter complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node;

establishing a second transport mechanism, the second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs;

filtering, at the security filter, the message traffic to bifurcate desirable message traffic from undesirable message traffic;

transmitting, via the network interface to a target node router serving the target node, a redirect message indicating that the target node router is to receive, via the second transport mechanism, the desirable message traffic directed to the particular target node and rerouted to the filter complex, the filter complex and the target node router conversant in the first transport mechanism and the second transport mechanism, the second transport mechanism defining a Virtual Private Network (VPN) protocol; and

directing, from the network management server, the filter complex to transmit, via the second transport mechanism over the communications network, the desirable message traffic to the target node, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

37. (Currently Amended) A computer program product having an encoded set of processor based instructions on a computer readable storage medium operable to store computer program logic embodied in computer program code encoded thereon for directing a processor to perform steps for redirecting network message traffic comprising:

computer program code to receive an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

Deleted: for receiving

computer program code to reroute all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic, rerouting all message traffic further comprising propagating, via a standard protocol corresponding to the first

Deleted: for rerouting

transport mechanism, a node address other than the node address corresponding to the target node, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filter complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node;

computer program code to establish a second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs; and

Deleted: for establishing

computer program code to direct the filter complex to transmit, by redirecting the desirable message traffic via the second transport mechanism over the communications network, the desirable message traffic to the target node, the redirecting thus transporting a particular message in the desirable message traffic via both the first transport mechanism and the second transport mechanism, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism, the second transport mechanism defining a Virtual Private Network (VPN) protocol.

Deleted: for directing

Deleted: the same message

39. (Currently Amended) A network management server for redirecting undesirable message traffic comprising:

means for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

means for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filter complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node;

means for establishing a second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs; and

means for directing the filter complex to transmit, by redirecting the desirable message traffic via the second transport mechanism over the communications network, the desirable message traffic to the target node, the redirecting thus transporting a particular message in the desirable message traffic via both the first transport mechanism and the second transport mechanism, the second transport mechanism corresponding to a virtual private network operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network, the second transport mechanism defining a Virtual Private Network (VPN) protocol.

Deleted: the same message

40. (Currently Amended) A method of redirecting an inundation of undesirable message traffic in a computer network comprising:

establishing, in the computer network, a first protocol for routing message traffic in the computer network;

Deleted: general

establishing, in the computer network, a second protocol specific to a virtual private network (VPN), the second protocol having a separate set of routing tables in an overlay arrangement with the first protocol, the second protocol having transport ability between at least a filter complex, a target node, and a target node router, the target node router included in a routing path to the target node, the target node router in communication with the target node via both the first protocol and the second protocol and operable to deliver the message traffic to the target node via either the first protocol and the second protocol;

identifying an indication of undesirable message traffic directed to the target node via the first protocol in the computer network;

Formatted: Indent: First line: 18 pt

propagating routing information according to the first protocol, the routing information operable for redirecting a message in the message traffic by designating the filter complex in the routing path to the target node via routing in the first protocol; and

Deleted: the

sending a reroute message to the filter complex, the reroute message operable to designate the target node as the destination of the message according to the second protocol, redirecting including sending instructions to the target node router coupled to the target node, the instructions designating the target node router as a destination router for the target node according to the second protocol,

the redirecting thus transporting the message via both the first protocol and the second protocol.

Deleted: same

41. (Currently Amended) The method of claim 40 wherein the first protocol and the second protocol~~s~~ being different protocols recognized in a Multi-Protocol Layer Service (MPLS) network.

42. (Currently Amended) The method of claim 19 wherein the first and second transport mechanisms are first and second protocols, the first protocol and the second protocol~~s~~ being different protocols recognized in a Multi-Protocol Layer Service (MPLS) network.

Formatted: Font color: Blue
Deleted: mediums
Formatted: Not Strikethrough

Allowable Subject Matter

2. Claims 1-5, 7-13, 16-23, 25, 27-37, and 39-42 are allowed.

The following is an examiner's statement of reasons for allowance: Any prior art of the record does not teach or suggest alone or in combination with other prior art of record the specific features required in the independent Claims 1, 19, 36, 37, 39, and 40 such as "the second routing transport mechanism is a virtual private network (VPN) protocol having a separate set of routing tables in an overlay arrangement with the first, primary network protocol under which the rerouting to the filter complex occurs." The prior art taken either single or in combination fails to anticipate or fairly suggest the above limitations of applicant's independent claims in such a manner that a rejection under 35 U.S.C. 102 or 103 would be proper. Therefore, the claimed invention is considered to be in condition for allowance as being novel and non-obvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Contact Information

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/B. N. T./
Examiner, Art Unit 2135
04/04/2208
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135